

17257

July 21, 2020

[Insert mailing address]

Dear [Name],

We are writing to let you know about a data security incident that may have involved your personal information. The Springfield Museums takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

#### What Happened

We were recently notified by Blackbaud, one of our third-party service providers, of a security incident. At this time, we understand Blackbaud discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

#### What Information Was Involved

It's important to note that the cybercriminal **did not access your credit card information, bank account information, or social security number**. However, we have determined that the file removed may have contained your **Massachusetts Driver's License Number**. Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, their research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

#### What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents. First, they were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating

efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

#### What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the following law enforcement authorities: Massachusetts Office of Consumer Affairs and Business Regulation (617) 973-8787, 501 Boylston St, Suite 5100, Boston, MA 02116 and Massachusetts Attorney General's Office Call us in Springfield (413) 784-1240, 1441 Main Street, 12th Floor, Springfield, MA 01103. Ypu may also file a police report.

#### For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact me at (413) 314-6458 or [hcahill@springfieldmuseums.org](mailto:hcahill@springfieldmuseums.org).

Sincerely,

Heather A. Cahill  
Director of Development